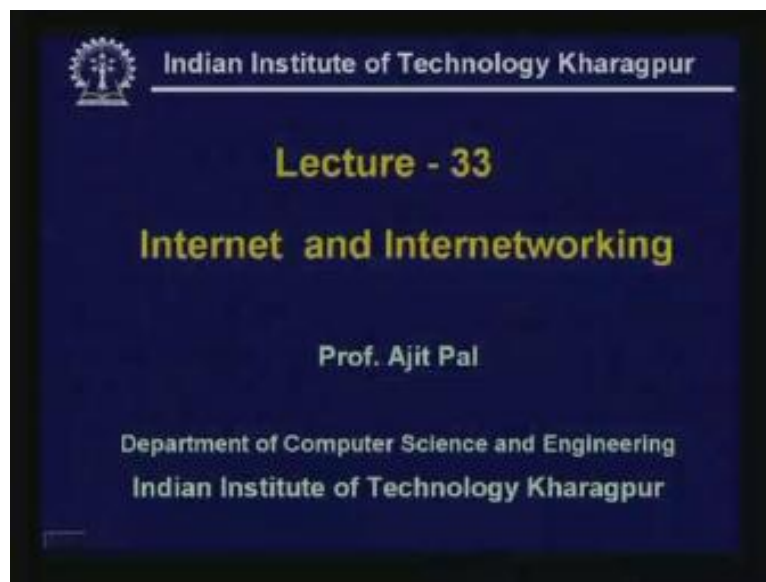


Data Communications
Prof. A. Pal
Dept. of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

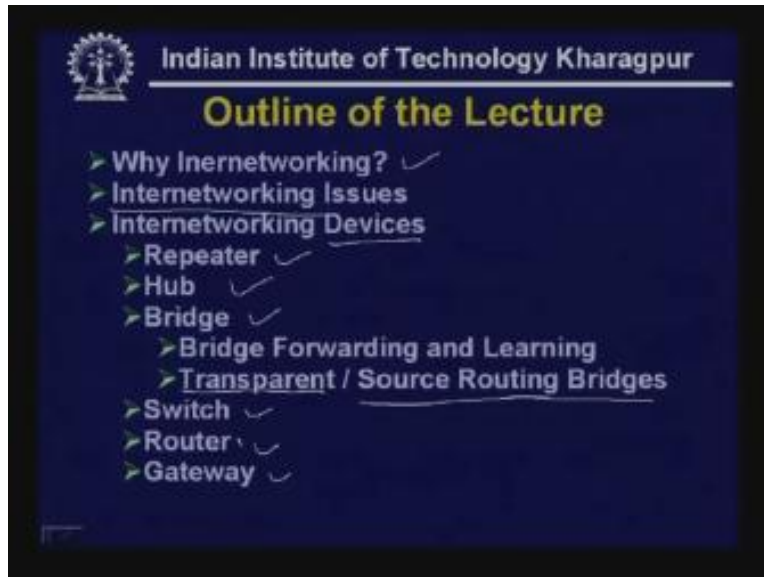
Lecture - 33
Internet and Internetworking

Hello and welcome to today's lecture on internet and internetworking. Here is the outline of today's lecture.

(Refer Slide Time: 01:02)



(Refer Slide Time: 02:05)



After a brief introduction I shall discuss about why internetworking, why at all internetworking is needed, and then I shall discuss various issues related to internetworking. Also, you will see that it will involve two types of devices, two types of components; one is hardware, another is software and in this lecture I shall focus on the hardware components which are essentially internetworking devices and there exist various types of devices such as repeater, hub bridge, bridge of different kinds like there is some bridge which does forwarding and learning which are known as transparent bridge, then source routing bridge and then there are switches, routers and gateways so I shall discuss all of them one after the other.

(Refer Slide Time: 02:39)

Indian Institute of Technology Kharagpur

Lecture 33: Internet and Internetworking

On completion, the student will be able to:

- Specify the need for internetworking ✓
- State various issues related to internetworking ✓
- Explain the operation of various internetworking devices:
 - Hubs ✓
 - Bridges ✓
 - Bridge forwarding and learning
 - Transparent and source routing bridges ✓
 - Switches ✓ Routers ✓ Gateways ✓

And on completion, the student will be able to specify the need for internet working, state various issues related to internetworking and they will be able to explain the operations of various internetworking devices like hubs, bridges, transparent and source routing bridges. These transparent bridges uses bridge forwarding and learning, they will also be able to explain about the switches, routers and gateways.

(Refer Slide Time: 04:06)

Indian Institute of Technology Kharagpur

Introduction

Point-to-Point

RS232C

Possible Communication Approaches

Switched-Communication Network (WAN)

*Telephone Network
X.25
Frame Relay*

Multipoint Broadcast Network (LAN)

Let us look at the possible communication approaches. We have discussed different types of communication systems in the last 32 lectures and in these 32 lectures we have discussed various communication approaches.

First one is point-to-point. We have seen how two stations can communicate with each other with the help of point-to-point league such as RS – 232C, then we have discussed different types of switched communication and network which is also known as WANs Wide Area networks, for example telephone network, X.25 frame relay and so on. These are essentially switched communication networks.


We have also discussed multipoint broadcast network like LAN, satellite networks then your cellular telephone networks, these are essentially multipoint broadcast networks. Thus, these are the three possible communication approaches we have already discussed in detail.

(Refer Slide Time: 04:47)



The LAN technology is designed to provide high speed communication over a small geographical area. So if you look at each of them separately we will find that the function of LAN is very limited over a small geographical region. On the other hand, WAN technology is designed to provide communication across different cities, countries and continents but their rate of data transfer is not very high and it has been absorbed that isolated LAN and WAN have limited potential and usefulness. So unless these LANs and WANs are interconnected together they are able to exchange information with one another. This isolated LANs and WANs are of not much use so this has led to what is known as internetworking.

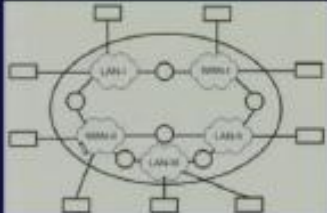
(Refer Slide Time: 06:57)

 Indian Institute of Technology Kharagpur

The Internet

➤ The basic objective is to connect individual heterogeneous networks, both LAN and WAN, distributed across the world using suitable hardware and software in such a way that it gives the user the illusion of a single network.

This single virtual network is widely known as **internet**, which is a **network of networks**.

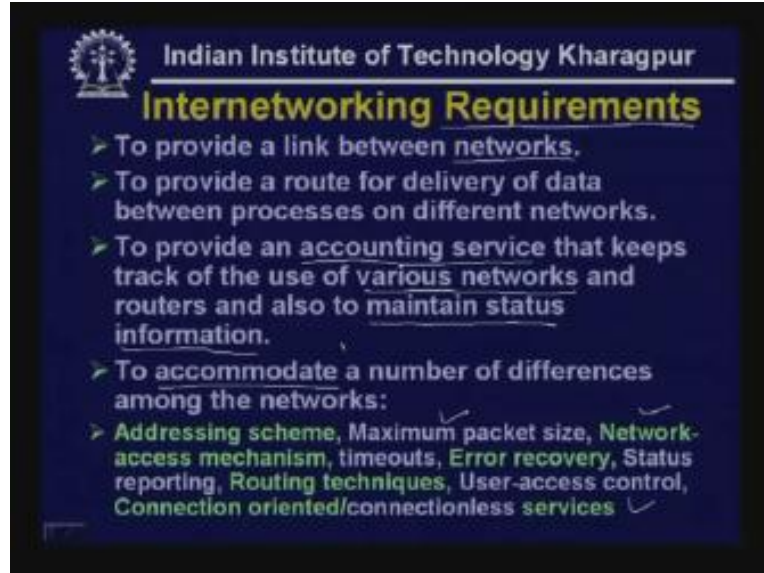


What is internet? The basic objective **of internet** is to connect individual heterogeneous network of both LAN and WAN distributed across the world using suitable hardware and software in such a way that it gives the user the illusion of a single network.

So far as the user is concerned it will be communicating through a number of systems such as LANs, WANs but it will be transparent to them, they will be able to communicate seamlessly and that is the objective of internet. This single virtual network is widely known as internet which is essentially a network of networks.

As you can see in this diagram we have several LANs such as LAN1, LAN2 and a number of WANs Wide Area Networks like WAN1, WAN2, LAN3 you see several LANs and WANs are interconnected together and these form the internet. Here are the users of stations connected to different LANs and WANs to them. Whatever is within this circle is transparent that means they can communicate with each other irrespective of whether it is passing through this LAN and through this WAN which is in this particular station communicating through WAN2, LAN3 then LAN2 so this will be transparent to it. That is the objective of internet and the way it is being done is known as internetworking.

(Refer Slide Time: 11:14)



So let us have a look at the various requirements for internetworking. First objective is to provide link between networks. You have got isolated networks, LANs and WANs you would like to link them together and link between these networks to provide a route for delivery of data between processes on different networks. That means processes running on different networks has to be provided a route so that from one network it can be transferred or delivered in another network.

Moreover, another requirement is to provide an accounting service that keeps track of the use of various networks that means a particular network may be using two LANs and Wide Area Networks and for some of them one has to pay so some accounting is necessary **and routers and also to maintain status information. So apart from** keeping track of what is going on some status information is maintained so that the users or stations can know what is going on and if there is anything wrong they can get the information. Then another requirement is to accommodate a number of differences among the network so wherever you interconnect a number of LANs and WANs of heterogeneous type it is quite natural they will be having many differences. Let us see what possible differences that exist.

First one is addressing schemes. We know that for local area network we have discussed the addressing scheme. The Ethernet LAN uses 48-bit MAC address but in other network it can be different. We have already discussed the token ring and token bus networks they are addresses but not the same as the Ethernet so the addressing scheme may be different in different networks and different LANs and WANs.

Then we have the packet size. The packet size of different networks can be different. In one case it can be 15000 bites but in other cases it can be 64 kilo bites. Thus, the packet size can vary from network to network. Then we have the network access mechanism.

We have discussed various medium access control techniques and we have seen that the medium access control techniques used in different networks are indeed different so in spite of these differences communication is possible.

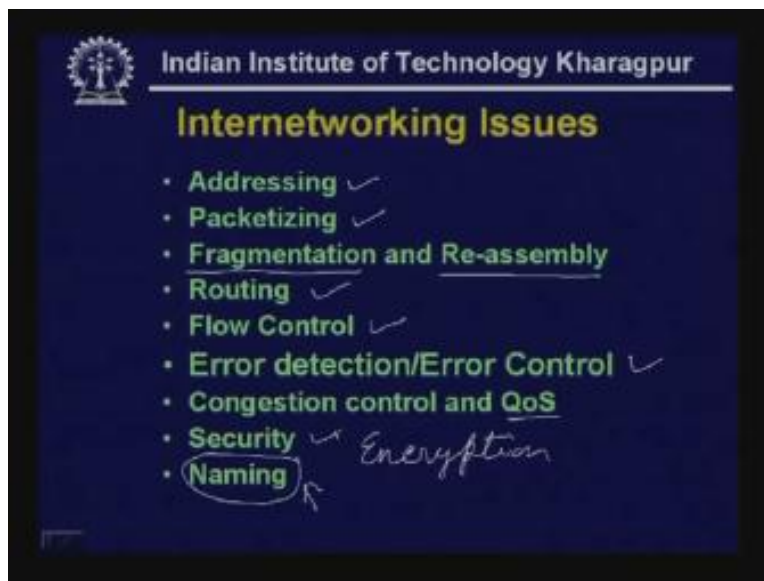
Time-outs: time-outs means as the packet passes through the network it is not allowed to stay in the network for a very long time some time-out is maintained and those times will be different in different networks.

Error recovery: We have seen that when you are passing a particular packet through a network or a number of networks there is a possibility of error so whenever an error occurs you have to recover from the error situations that are your error recovery that can be different in different networks.

Status reporting also can be different in different networks. We have discussed various routing techniques like fixed routing, adaptive routing and so on. Routing approaches can be different in different networks.

User access control can be also different in different networks. It can be connection oriented or datagram type of service. So, services can be different. In spite of all these differences the objective of the internet is to communicate between two stations in a transparent manner and obviously the objective of internetworking is to accommodate all these differences.

(Refer Slide Time: 13:31)



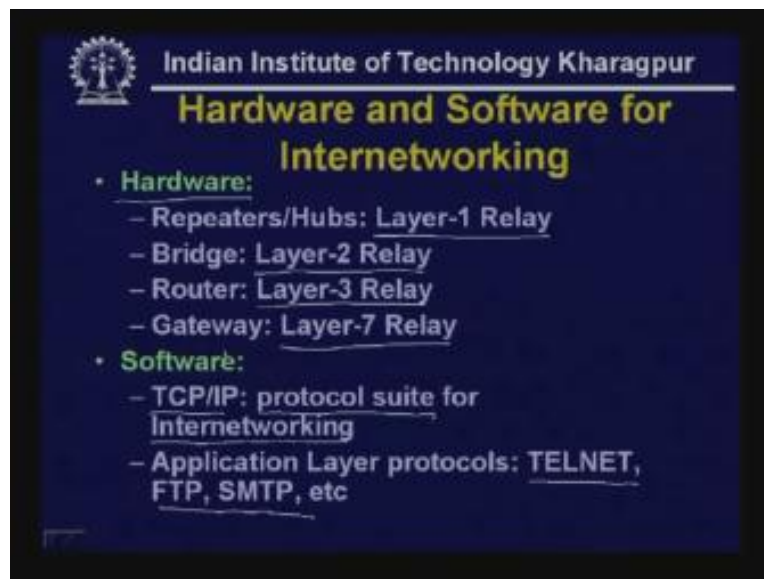
Now let us have a look at the various internetworking issues. First one is addressing. We have seen that, whenever two stations want to communicate with each other they must have some address and in case of internet we have seen the 48-bit medium access control MAC address.

In other networks this addressing scheme can be different. So we have to discuss about addressing then we have to do packetizing. Apart from data other information like source address, destination address and various other things have to be put together in the form of a frame known as packetizing.

As we have seen the packet size can pass through a network cannot be same so it may be necessary to fragment, that is, divide a particular packet into a number of packets as it goes through a network then at the other end or in the destination node they have to be put together they have to be reassembled. So it will be necessary to perform fragmentation and reassembly then you have to do the routing as the packet passes through a sequence of networks.

Then for the purpose of the reliability it will be necessary to do flow control, error detection and error control, it will be also necessary to perform congestion control and to ensure quality of service. then other issues like security, network security has to be maintained as the data passes through the network, security has to be maintained with the help of suitable encryption decryption technique then it is sometimes necessary to use names instead of addresses because it is difficult to memorize or remember the names so sometimes it will be necessary to use address and then we have to see how the naming is being done and how actually mapping from name to address is performed. So these are the various internetworking issues we have to discuss.

(Refer Slide Time: 15:22)

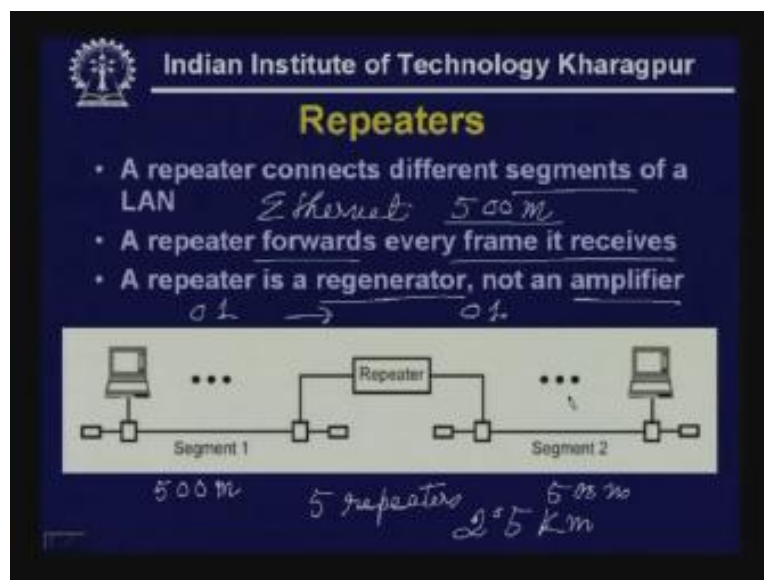


First we shall focus on the various types of hardware and software needed for this purpose. we will see that we have to use different types of hardware such as repeaters and hubs which are essentially layer - 1 relay, they act as some kind of relay, then bridge and switches they are layer - 2 relay then router which are layer - 3 relay and gateway which can operate in all the layers which is layer seven relay so these are the different hardware components we have to use when we do internetworking.

On the other hand you will require software. The most common software that is used today is TCP/IP Transmission Control Protocol and Internet Protocol it operates in two layers. There are four layers but TCP/IP essentially operates in two layers as TCP in the transport layer and IP in the network layer and it's a protocol suite for internetworking.

This TCP/IP acts as glue and which binds all different types of networks into one. So TCP/IP is the software which acts as a glue which actually puts different networks together into one network. And of course there are application layer protocols which operate on top of TCP/IP like TELNET, FTP, SMTP etc. So we will require some hardware and some software. In this lecture we shall mainly focus on hardware and in the next two lectures we shall focus on TCP/IP.

(Refer Slide Time: 19:03)



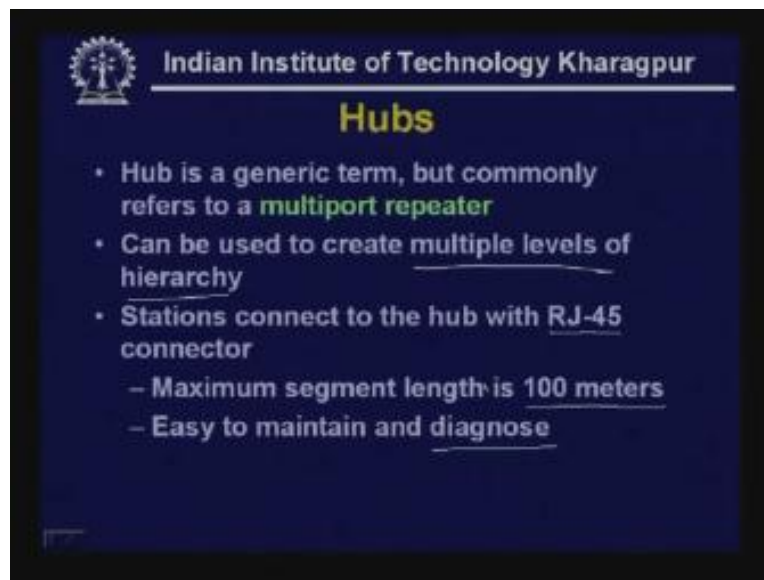
So first let us consider repeater. A repeater connects different segments of a LAN. We have seen that there is a maximum length of a segment of network. For example, if you are considering Ethernet then we know the maximum segment length of 802.3 Ethernet 500 m but if you want to have a single network with network span of more than 500 m then you have to use a device known as repeater in between two segments. So here we see we have got two segments each of them can be of 500 m, this is 500 m and this is 500 m so if you put them together you get 1 km of Ethernet LAN and as you can see these two segments are linked by a device known as repeater. So what the repeater does is it forwards every frame it receives. So if it receives a frame on this segment it forwards it to segment two, if it receives a frame on this segment it forwards it to segment one so in this way it does the forwarding.

You may be asking is it a amplifier or in what way it differs from amplifier? Actually a repeater is not really an amplifier. What an amplifier does is it amplifies the signal as well as the noise and it does discriminate between signal and noise. On the other hand, a repeater essentially extract the signal, removes the noise and regenerates the signal. That

means if you are sending a sequence of zeros and ones on this side then it may get submerged in noise but it will remove the noise and extract these bit sequences and then regenerate it, it brings the voltage levels corresponding to 0 and 1 and puts them on the other side. So this way it is not really an amplifier but it is a regenerator. That means on this side the noises are not transferred, if you are sending from this side to this side the noises are not transferred but the bit sequences are transferred in regenerated form. So it is a bidirectional link. The transfer of bits can take place from this side to this side as well as from the other side to this side, segment one to segment two and segment two to segment one. So, repeater is a very useful device for expanding a LAN.

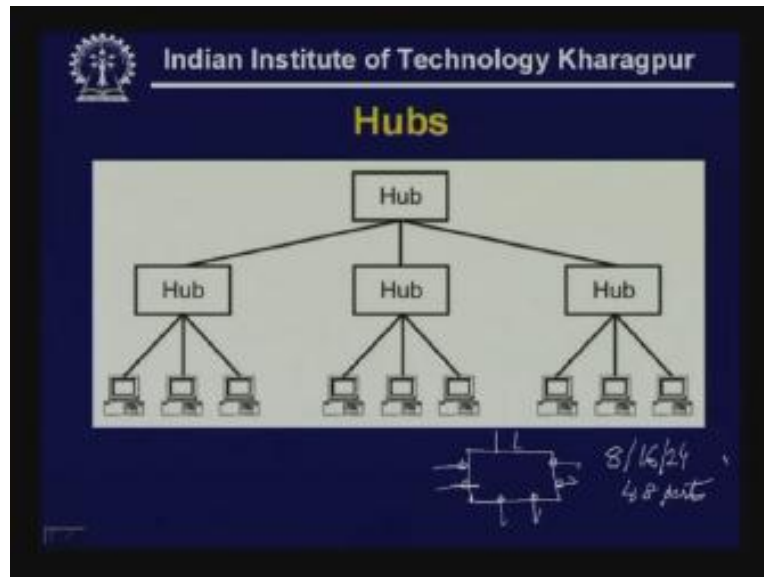
Hence, you are not really connecting two LANs by a repeater but essentially you are increasing the span of a local area network. As you know, in case of Ethernet you can have five repeaters at most in cascade so in that way maximum network span can be 2.5 km. so you will require a sequence of repeaters so before the signal level is becomes very poor becomes very difficult to extract from noise you have to put repeater. So repeaters are a very useful device for increasing the size of networks.

(Refer Slide Time: 20:12)



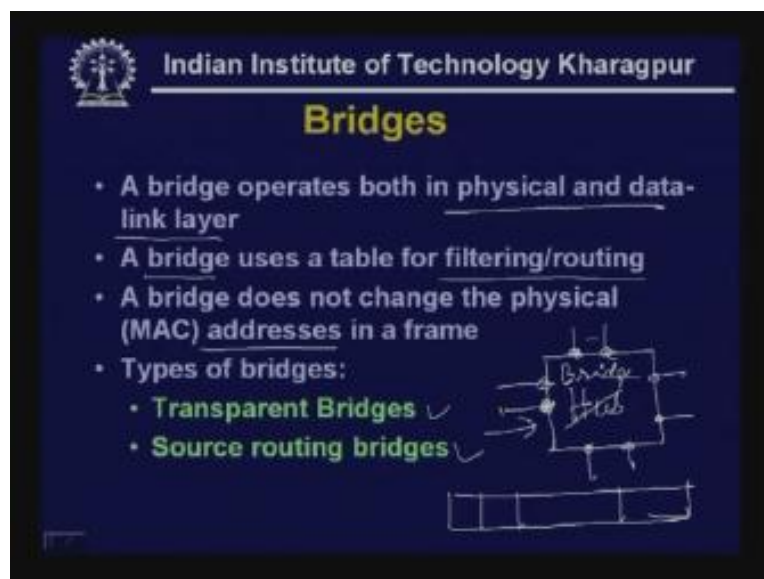
Another version of repeater is usually called a hub. Hub is a generic term which means from where signals are generated and received. But here by hub we commonly refer to a device known as multiport repeater, essentially it is a multiport repeater. We have seen in the previous diagram a repeater has got two ports; here you have got one port, another you have got another port so it linking the two segments but a hub can have multiple ports so it can be used to create multiple levels of hierarchy with the help of a hub, you can create a single LAN having multiple levels of hierarchy and stations connect to the hub usually with the help of RJ-45 connector and as we have already discussed maximum segment length is 100 m so it is easy to maintain and diagnose that means detection is easy. That's why this type of topology is becoming more and more popular.

(Refer Slide Time: 21:15)



Here you have got a hub at the upper level so this is connected to three different ports here although it is shown that it is connected to a single port essentially a hub has got multiple ports. This is a port, this is a port, this is a port (Refer Slide Time: 20:40) this is a port, this is a port and this is a port so these three hubs are connected to three different ports here. Then in the second level there are a number of stations or computers connected to different ports of the hubs. So it is essentially a multiport repeater and you can see how in a heretical manner you can expand a network and create a big network with large number of computers. Usually hubs are available with 8 ports, 16 ports, 24 ports and nowadays 48 ports.

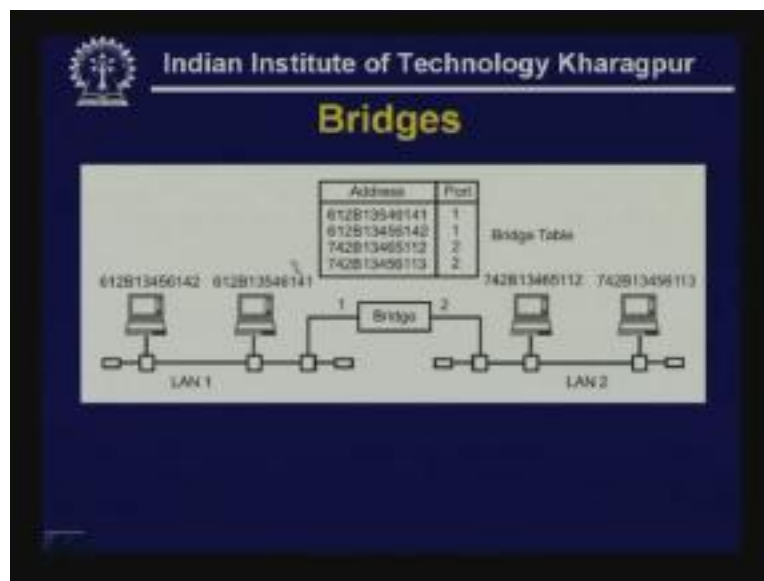
(Refer Slide Time: 23:15)



Now the second device that we shall discuss is bridges. A bridge operates both in physical and data-link layer. We have seen, in case of repeaters it does not do any filtering. Whatever is received on a port, say this is a hub let's assume (Refer Slide Time: 21:44) and you have got a number of ports, 8 port is here so whatever signal is on this port will be available on all other ports, it is repeated on all ports. So as a result hub is some kind of a dumped device, it does not do any filtering except regeneration of the signals and same signal is repeated in all other ports so it does not do any filtering or routing.

On the other hand, a bridge uses a table for filtering and routing. That means if a packet arrives here a bridge will not forward it to all other ports which is done by hub a hub forwards the packet on all the ports but a bridge does not do that. However, the bridge does not change the physical addresses in a frame. Thus, as we know a frame will have the source address, destination address, data, CRC and so on so various parts will be there in a frame and it does not change the content but it does the filtering or routing we may call it routing as well. There are two types of bridges; one is known as transparent bridge and another is known as source routing bridge. Let us see the operations of these two types of bridges.

(Refer Slide Time: 23:25)



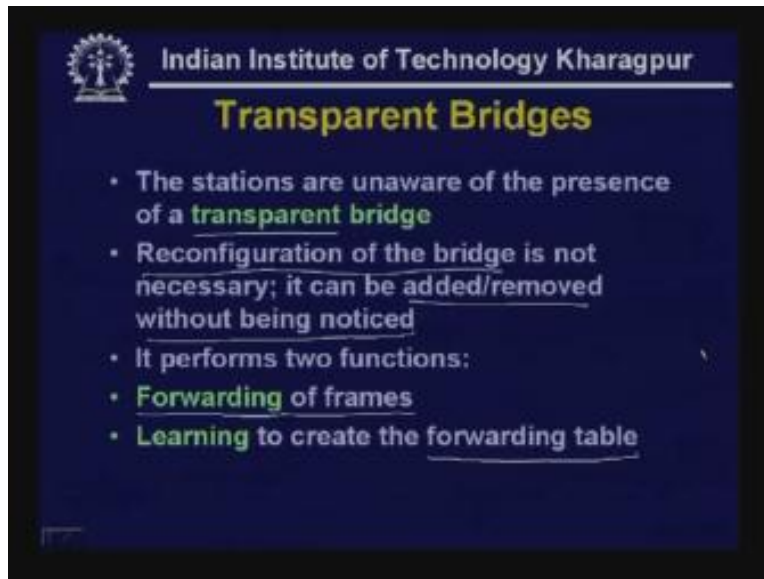
So here the operation of a bridge is shown. Here as you can see these are the 48-bit Mac addresses represented in hex form is shown here. In this particular case a bridge is shown with two ports but as I said a bridge can have many ports. So on this port one a LAN – 1 is connected to which two stations are connected with the Mac addresses as given so port one and address so a table is maintained, address and port number.

On port two again two other stations are connected with these addresses 742B and so on and 742B and so on, this is 112 and 113 (Refer Slide Time: 24:15) so this is connected to

port two, this kind of table is maintained in a bridge and this table is used for the purpose of filtering or you may call it routing.

The functions of the transparent bridge: All stations are unaware of what is going on inside the bridge, it acts as some kind of plug and play device, a bridge is installed, there is no need to do any reconfiguration, any initialization nothing is required, simply plug it and then it will start operating and that table will be automatically created.

(Refer Slide Time: 25:09)



So, reconfiguration of bridge is not necessary, it can be added and removed without being noticed. And question arises how it really works so that it behaves like a transparent bridge. Actually it performs two important functions. First function that it does is known as forwarding of frames. This is the key function it performs. Another operation is known as learning which is necessary for forwarding to be done; this learning is done to create the forwarding table the table that I have shown just now.

(Refer Slide Time: 28:24)



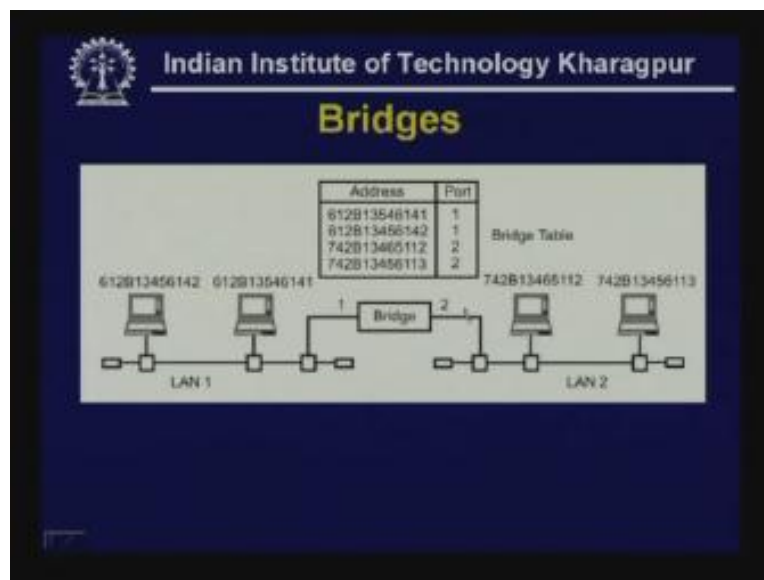
Indian Institute of Technology Kharagpur

Bridge Forwarding

- Discard the frame if source and destination addresses are same
- Forward the frame if the source and destination addresses are different and destination address is present in the table ✓
- Use flooding if destination address is not present in the table

What is being performed in bridge forwarding? It essentially performs three functions; discard the frame if source and destination addresses are same. That means if the source and destination addresses are same that means around the same port or on the same port.

(Refer Slide Time: 30:14)



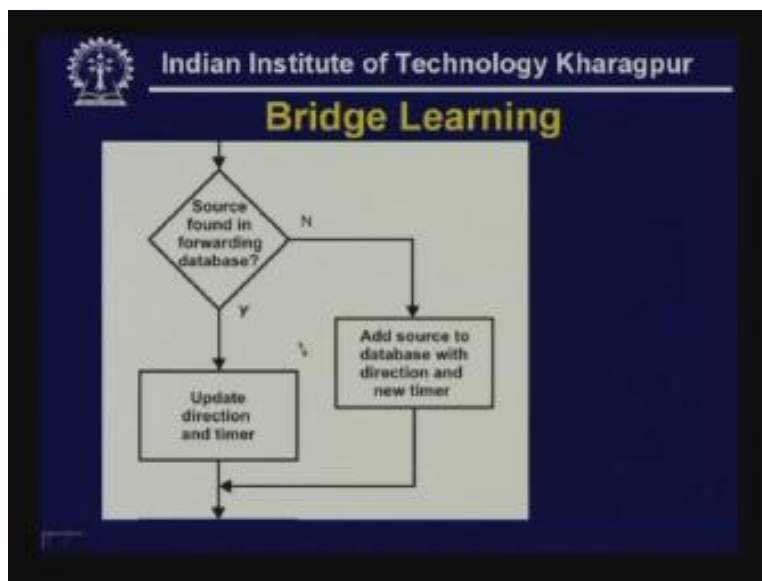
For example we have seen that these two addresses are connected to the same port and are on the same port. So, if a frame is generated on this destination address whether it is this or this on port one then what will happen is that particular packet, suppose this is sending a packet to this station (Refer Slide Time: 26:47) then the bridge will discard that

packet because it is directly communicated between this station to this station so it will not be forwarded to the other port of the bridge.

Second operation that is done is **forwarding** the frame, if the source and destination addresses are different and destination address is present in the table. Suppose the destination address corresponds to the other port and if this present here and the port number is known then it will simply forward it. Suppose this station is sending a frame with this destination address so this destination address is present in the table and it shows that it is on port number two so this frame is forwarded on port number two so this is how this works. So this is the second operation 'forward' forwarding the frame and the first one is 'discard'. Third is, a particular destination address may not be present in the table.

So, in the beginning whenever you plug a bridge in the network that table will be empty so in such a case there will be no destination address so in such a case what the bridge does is it forwards on all the other ports except from where it has come so this is known as flooding. So flooding is done and obviously it will be delivered to the destination address.

(Refer Slide Time: 30:26)

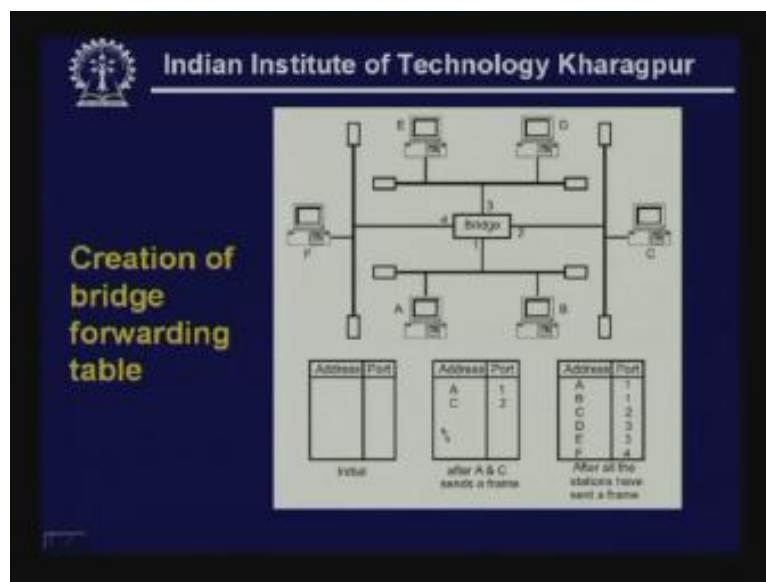


For successful operation of bridge forwarding the bridge learning process is performed. Here as you can see, if a particular station sends a packet the station's MAC address is automatically recorded in the table along with the port number. So source is found in forwarding database and if it is no then that source address is added to source address database with direction and new timer. It also maintains a timer. The reason for timer is, the table is not really static. The table that is being created keeps on changing with time. The reason for that is, suppose a particular station does not send any packet for a long time so it is something like that in such a case what will happen is after a few minutes it will see the condition of the timer and when the time-out occurs that station's MAC

address is removed from the table and whenever a frame is received then even when the frame MAC address is present in the database its timer is updated. So the direction is updated that means you can take out a station from one place for example here you can take out the station from here to there (Refer Slide Time: 30:02) then automatically after the station is connected to this side it sends the frame and automatically that table will be updated.

So apart from performing the building of the table it also maintains the timer and whenever the time-out occur those addresses are removed from the table so this is how bridge learning operation is performed. So, bridge learning and bridge forwarding together makes the transparent bridge operation.

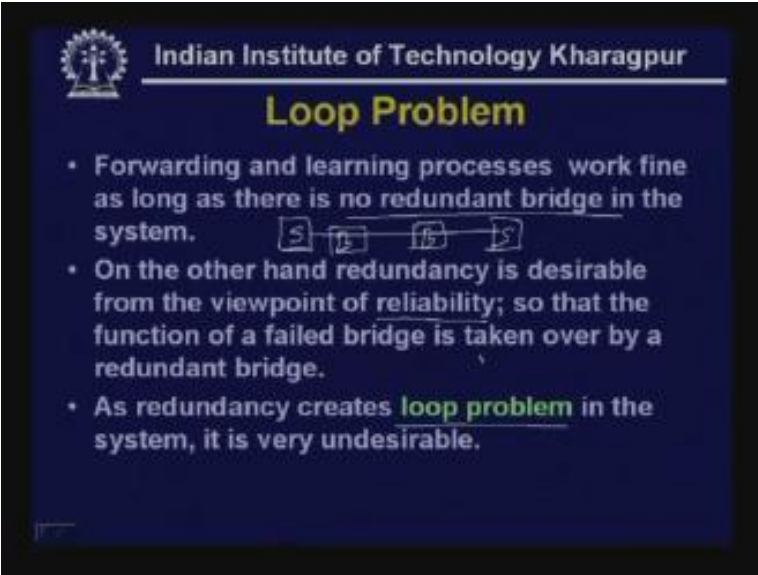
(Refer Slide Time: 30:57)



And here we can see how the bridge forwarding table is created. This is the initial condition, a bridge has been plugged in and it has been connected to four LAN's. This is LAN 1, this is LAN 2 this is LAN 3 and this is LAN 4 so it is connected to four LANs. Initially this table is empty. Now, whenever A sends a packet the bridge notices it and then it ((...)) the table, whenever C sends a packet it also notices it and will [su.....31:17] a table between A and C.

Essentially we have to write the 48-bit MAC addresses if it is Ethernet. So in this way in the long run all the stations if they are active their entries will come in the address along with the port number. So after all the stations have sent a frame this will be the situation of the table. I have not shown the timer here but the timer value is also maintained. And whenever suppose this C is turned off then automatically after some time this entry will be removed from the table. So this is how the bridge forwarding table is created in transparent bridge operation.

(Refer Slide Time: 33:34)



Indian Institute of Technology Kharagpur

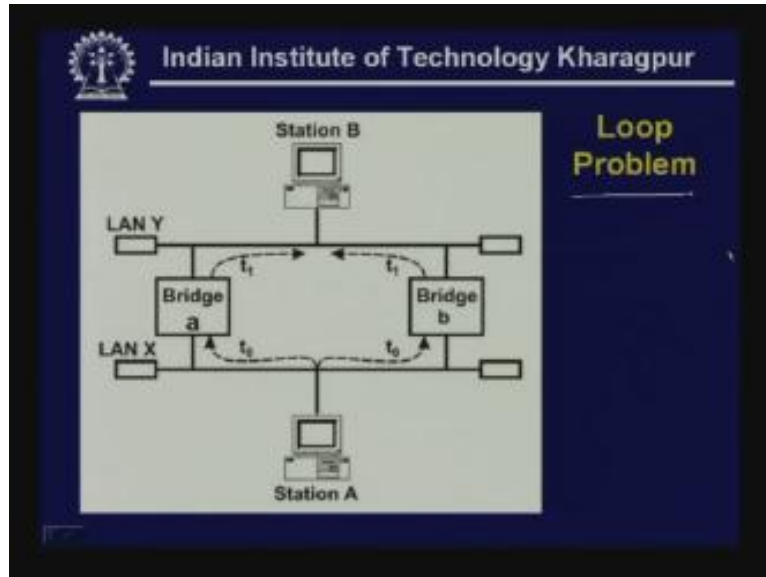
Loop Problem

- Forwarding and learning processes work fine as long as there is no redundant bridge in the system.
- On the other hand redundancy is desirable from the viewpoint of reliability; so that the function of a failed bridge is taken over by a redundant bridge.
- As redundancy creates **loop problem** in the system, it is very undesirable.

This forwarding and learning processes work fine as long as there is no redundant bridge in the system. So only there exist one path from one station to another and in such a case there is no problem. So, for unique path it is necessary that there is no redundant bridge so from one station to another station there is a unique path may be through a number of bridges. These are the bridges; this is one bridge, this is another bridge, this is a station and this is a station (Refer Slide time: 32:45). However, from the view point of reliability it is necessary to have multiple paths. The reason is if one bridge becomes faulty then the source stations will not be able to send if there is no redundant path. So, for the sake of reliability it is necessary to have redundancy.

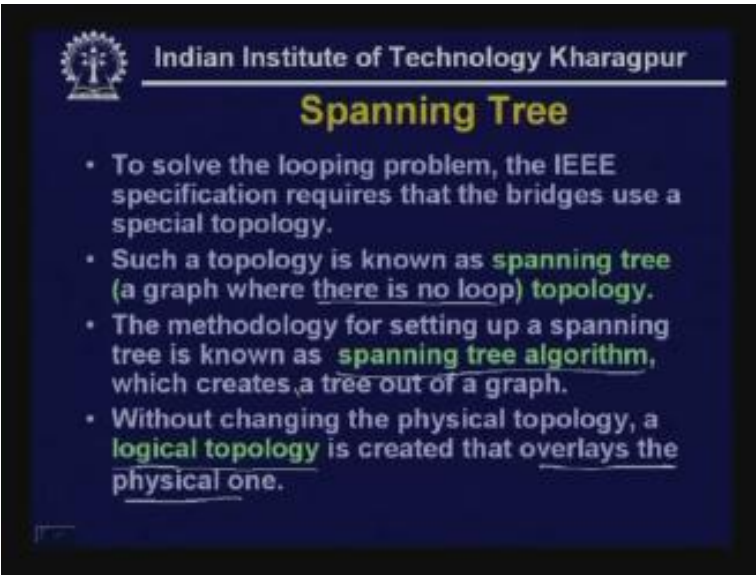
To get best of both the worlds that means the advantage of this transparent bridge and at the same time to avoid the problem of redundancy where redundancy creates loop problem so we have to avoid this loop problem and if you want to retain it then let us see how the loop problem arises.

(Refer Slide Time: 34:52)



So here you can see there are two LANs; this is LAN X and LAN Y and these are connected by two bridges bridge A and bridge B. Whenever station A sends a frame to bridge A and sends a frame on this network LAN X then bridge A as well as B bridge B receives it and since the destination address is not known it sends it to network LAN Y and also bridge a sends it to LAN Y. Now this t_1 (Refer Slide Time: 34:25) is received by LAN bridge B and again it forwards it to LAN X. So in this way some kind of loop occurs so the frame sent by station A goes to bridge B goes to LAN Y then it is forwarded by bridge A again it is forwarded by bridge B so in this way looping arises. So a frame can indefinitely keep on looping within the network before it is delivered. This is the typical loop problem and we have to avoid that loop problem. So loop problem can be avoided by using a technique known as spanning tree.

(Refer Slide Time: 35:39)



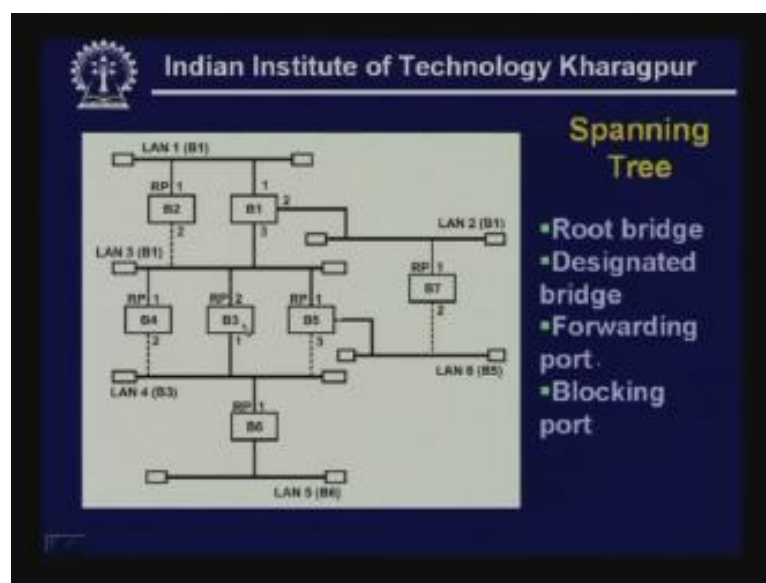
Indian Institute of Technology Kharagpur

Spanning Tree

- To solve the looping problem, the IEEE specification requires that the bridges use a special topology.
- Such a topology is known as **spanning tree** (a graph where there is no loop) topology.
- The methodology for setting up a spanning tree is known as **spanning tree algorithm**, which creates a tree out of a graph.
- Without changing the physical topology, a **logical topology** is created that overlays the physical one.

Spanning tree is essentially a special kind of graph where there is no loop. So a spanning tree topology is created. The methodology for setting up a spanning tree is known as the spanning tree algorithm. There exist standard algorithms efficient algorithms for creating spanning tree of a graph and we can use that for transparent bridge and without changing the physical topology. So some kind of logical topology is created that overlay on the physical one. Let us see how exactly it has been done here.

(Refer Slide Time: 38:59)



Here you see you have got LAN 1 to which two bridges are connected, you have got LAN 2 to which one bridge is connected, you have got LAN 3 to which three bridges are

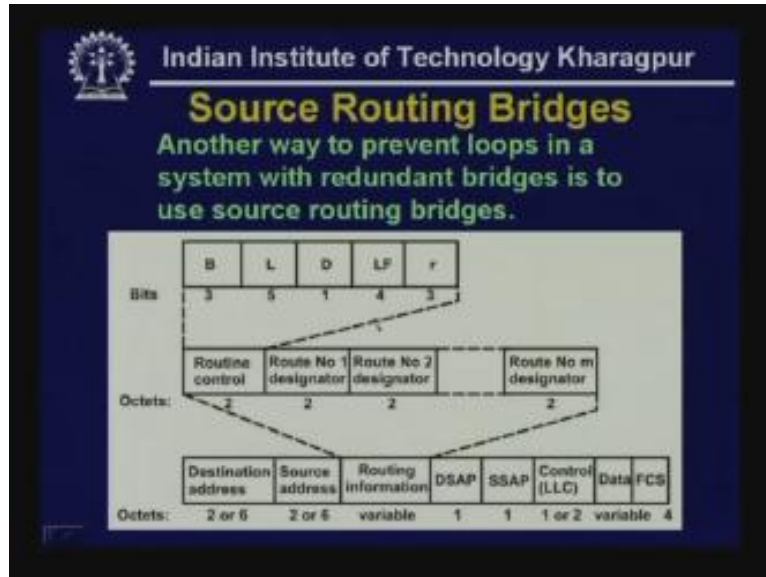
connected and LAN 4 and LAN 5 one bridge is connected so in this way you have got multiple paths and multiple bridges in this network which is connecting five different LANs. Now there is a spanning tree algorithm which identifies a root bridge, then it identifies the destination bridge and again it identifies the forwarding port and identifies the blocking port. I am not discussing the algorithm which makes use of these terminologies but the outcome is shown here. For example, this is the route bridge for LAN 1 actually if you have multiple bridges then the bridge having lower MAC address is used as the route bridge. So this is considered as the route bridge.

Here this particular path (Refer Slide Time: 36:51) is the blocking path. On the other hand, bridge B1 is where both the ports are forwarding ports. Then if you look at this bridge you can see this is the forwarding port and this is the blocking port so the dotted lines are blocking ports. That means these LANs are not used for forwarding purposes. Whenever you look do this then you find that from any LAN to any LAN there is a unique path.

For example, say from LAN 1 if you want to go to LAN 2 you have to only go through this bridge B1 and from LAN 2 to LAN 3 if you want to go you have to use bridge 7 then from bridge 7 it goes to bridge 1 then to bridge 2 then through bridge 1 it goes to LAN 3. Or if b this LAN 2 wants to communicate with some stations on LAN 5 so although there is a path like this instead of this path as you can see it has to be connected and forwarding will take place in this manner and the path is unique so there is a unique path the logical topology is created on the physical topology and dotted lines are not used for forwarding purposes they are blocked, that is the spanning tree approach.

However, if because of some reason suppose this particular bridge becomes faulty then automatically the spanning tree will be modified and some of these ports will become forwarding ports and both the ports will become the blocking ports. So in this way the spanning tree is created and using this spanning tree the transparent bridge will work.

(Refer Slide Time: 39:37)



Apart from these transparent bridges there is another routing technique that is used which is known as source routing. In this source routing the source itself decides the route that will be used by a packet through a number of bridges so all the intermediate bridge addresses are provided by the source stations.

The packet format is shown here. As we have seen normally the destination addresses and source addresses are provided. But in this particular frame as you can see apart from destination address and source address the routing information contains a number of other addresses. For example, route number one designator, route number two designator and route number m designator and so on. So with the help of these designators you can identify the route and also there are 16-bits for route control. The source station provides all the information for **routing through which** the packets will go one after the other and all the information is provided, it is quite simple. However, the source node has to gather all the information from other parts of the network before this packet can be framed and it can send the packet to the designated station.

(Refer Slide Time: 43:23)

Indian Institute of Technology Kharagpur

Fast Bridge **Switch**

- Ports are provided with buffer
- Switch maintains a directory:
 - #address - port#
- Each frame is forwarded after examining the #address and forwarded to the proper port#
- Three forwarding approaches:
 - *Smallest* **Cut-through** – no collision or error detection
 - *Medium* **Collision free** – no error detection
 - *Long* **Fully buffered** – both collision and error free frames are forwarded

Diagram: A central box labeled 'SWITCH' with four lines extending from it, representing ports. To the right, a diagram shows a frame structure with 'DA' (Destination Address) and 'CRC' (Cyclic Redundancy Check) fields, with an arrow indicating the flow of data.

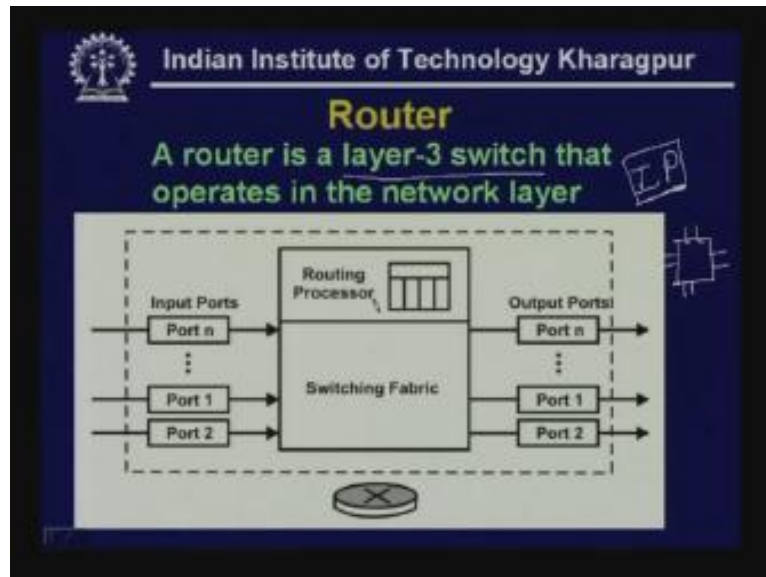
Switches: We have seen the function of a bridge. What is a switch?

A switch is nothing but a fast bridge. We have seen that a bridge performs the forwarding operation or routing function, may be done by software, but then it will be quite slow. Instead of doing by software it can be done by hardware and it can be done very fast and that is what is precisely done with switches and it uses the same technique as it uses a table or a directory having the address and port number and each frame is forwarded after examining the address and is forwarded to the proper port number.

I have already discussed about the three techniques; cut-through, collision-free and fully buffered. In cut-through the routing is done whenever a frame is received and only after receiving the destination address which is in the beginning of the frame the frame is transferred. On the other hand, to make a frame collision-free particularly in the context of Ethernet you have to receive at least 64 bytes so after receiving 64 bytes and if there is no collision then the frame is forwarded then we say that the frame is collision-free but error detection is not performed.

To perform error detection you have to receive the entire frame, compute CRC and after receiving the entire frame and computation of CRC if it is found to be error free then it is forwarded in the third case which forwards collision and error free frames. These are the three approaches used and obviously the cut-through approach has the smallest delay but it suffers from these advantages, it does not do collision detection and error detection. A frame can be forwarded which had suffered collision and which is not error free. Collision-free has got medium delay it will be sent only after receiving 64 bytes and fully buffered has long delay because it has to receive the entire frame, compute the CRC and then forward it.

(Refer Slide Time: 44:39)



Now, coming to the third layer that is the router the layer - 3 switch the routers operates in layer - 3 switch and obviously the addresses that is being used is IP address which I shall discuss in detail in the next lecture.

This is the schematic diagram of a router. As you can see a router has got a number of input ports so the basic configuration is the same. It has got a number of ports as input ports and output ports as shown here. But to the outsider the ports are essentially bidirectional. However, for the purpose of understanding the functionality we see that it has got a number of ports and there is a routing processor, there is a switching fabric which is a special piece hardware which can perform translation from one side to another very quickly. This is the switching fabric (Refer Slide Time: 44:31) and on the other side also you have got a number of output ports. This is the schematic diagram for a router which performs the routing of packets in layer - 3.

(Refer Slide Time: 45:20)



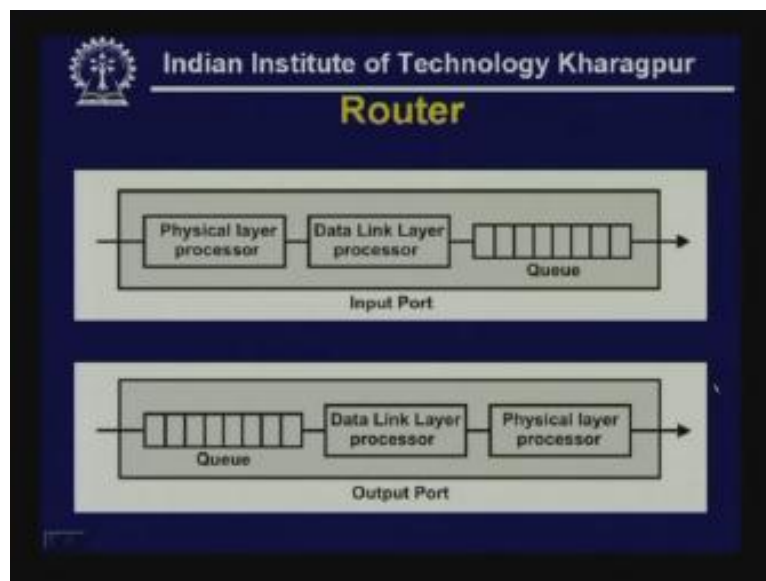
Indian Institute of Technology Kharagpur

Router

- A router has four basic components: **Input ports**, **output ports**, the **routing processor** and the **switching fabric**.
- **Input port** performs physical and data-link layer functions of the router. The ports are also provided with buffer to hold the packet before forwarding to the switching fabric.
- **Output ports** perform the same functions as the **input ports**, but in the reverse order.
- The **routing processor** performs the function of the **network layer**. The process involves **table lookup**.
- The **switching fabric** moves the packet from the input queue to the output queue by using specialized mechanisms.

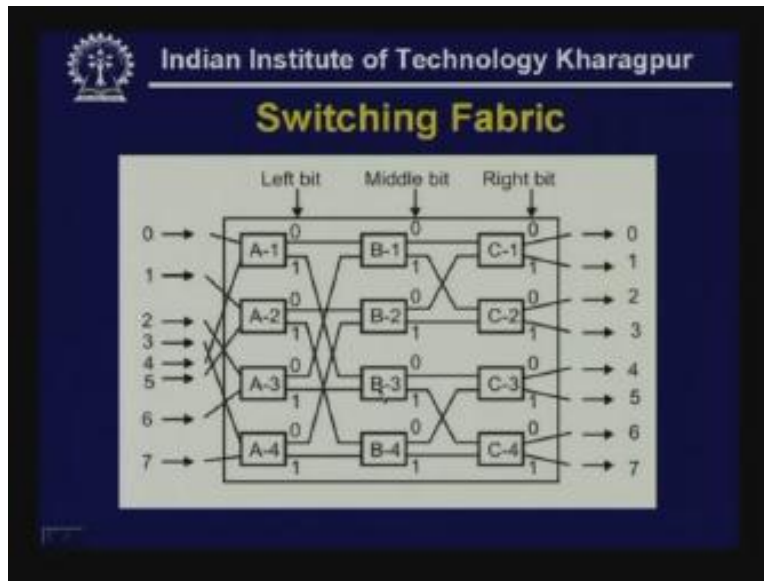
As we have seen a router has got four basic component input port it performs physical it performs physical and data link layer functions of the router the ports are also with buffer to hold the packet before forwarding to the switching fabric output port performs the same function as the input ports but it does it in the reverse order the routing processors performs the function of the network layer the processors process involves table lookup as we have already seen and the switching fabric moves the packet from the input queue to the output queue by using specialized mechanism and these are the two different functions shown here.

(Refer Slide Time: 45:58)



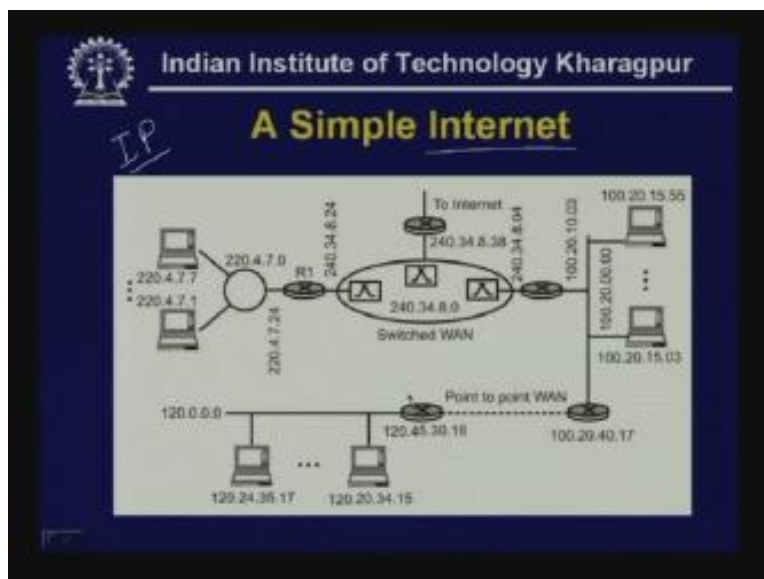
So here the input port receives from the packet from the physical layer processor and then it does the data link layer for processing there is data link layer processor then it maintains a queue before it can be transmitted. Similarly, whenever a packet goes to the output a queue is maintained then data link layer processor does the processing then it goes to the physical layer processor before it is launched on the transmission media.

(Refer Slide Time: 46:13)



And here is a typical switching fabric that is used. This is the special piece of hardware which moves the packet input to the output very quickly.

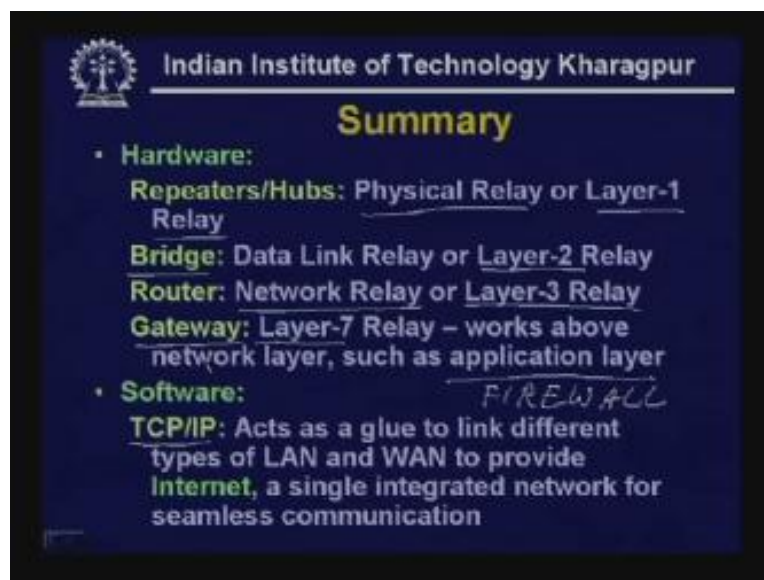
(Refer Slide Time: 47:34)



Here a simple internet is shown where you have got a ring LAN, a switched Wide Area Network WAN, a Local Area Network LAN bus type Local Area Network, there are two point-to-point links between two WANs Wide Area Networks and here you have got another LAN.

You will notice that here (Refer Slide Time: 46:54) whenever the internetworking is being done we have given a different kind of notation 240.34.8.24 what are these we have not yet discussed, these are essentially IP addresses that is been used in internetworking which is part of the TCP/IP. In the next lecture I shall discuss about the use of this type of IP addresses which is used when you do internetworking and data is transferred from one LAN to another LAN through a wide area network or between two wide area networks.

(Refer Slide Time: 49:40)



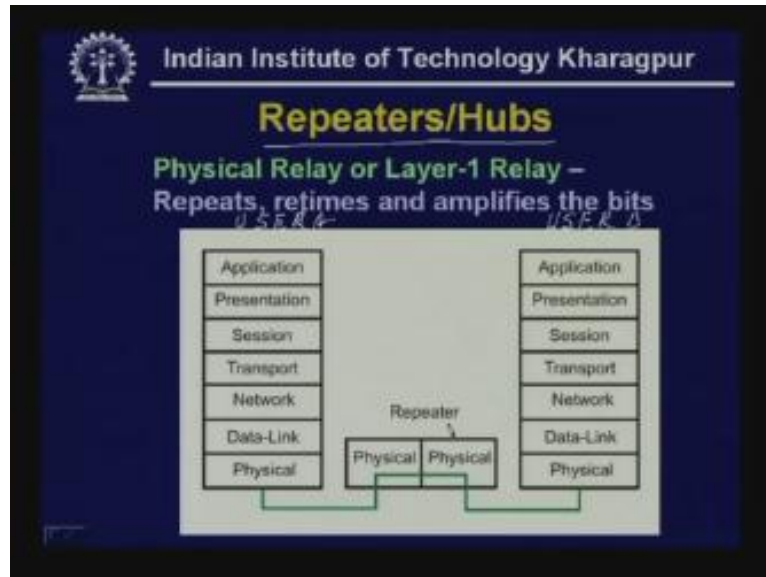
Here is the summary of what we have discussed today. We discussed about three different pieces of hardware, one is your repeater or hubs which operates in physical layer or which can be considered as layer - 1 relay, then we have discussed bridge which operates in data link layer which can be considered data link relay or layer - 2 relay then router which operates in network layer so it can be considered as network layer - 3 relay.

Another type of hardware which I have not discussed is known as layer seven relay. This works above the network layer such as application layer. This kind of gateway can be necessary. that means it will not only operate in layer - 2 or layer - 3 that means routing is not only performed based on MAC address or IP address, it can check the contents of data for example the content of an e mail so that kind of application gateway may be necessary in implementing fireworks for the purpose of security.

Although for normal routing purposes gateway is not necessary but in special situations such as implementing firewall for the purpose of security this kind of device will be necessary which operates in layer 7 that means it operates in application layer, it can look

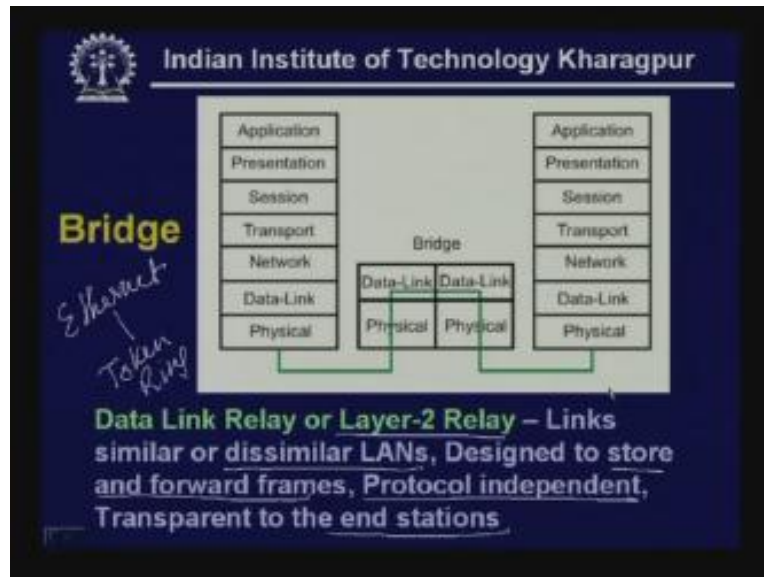
at the contents of data. Then we have the software which acts as a glue to link different types of LAN and WAN to provide internet a single integrated network for seamless communication.

(Refer Slide Time: 50:37)



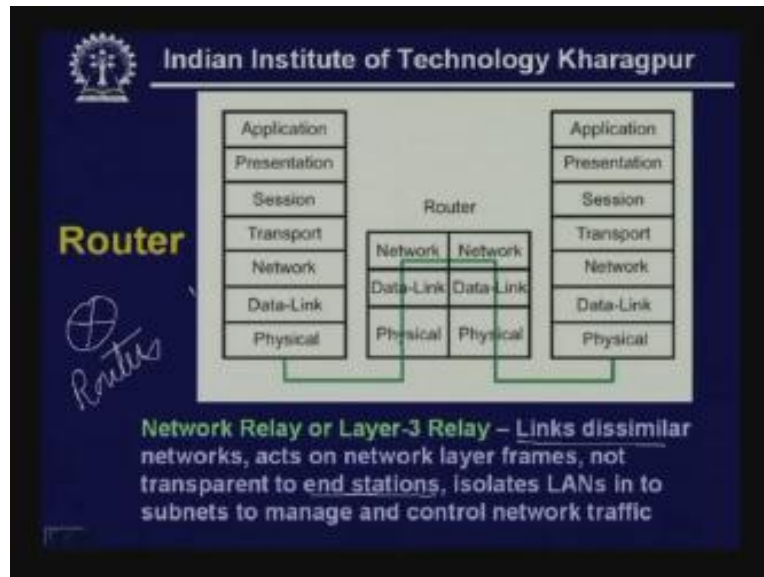
And here it gives some kind of a pictorial representation of the layer - 1 relay the functions of repeaters and hubs. as you can see this is one system say user A and here is another system say user B or station A station B they where communicating with each other and here you have got a repeater in between. So, repeater essentially performs bit by bit translation so it receives bit by bit regenerates it and transfers bit by bit so it is operating in the physical layer and this is connected to user A as well as it is connected to user B and communication is taking place in physical layer.

(Refer Slide Time: 51:55)



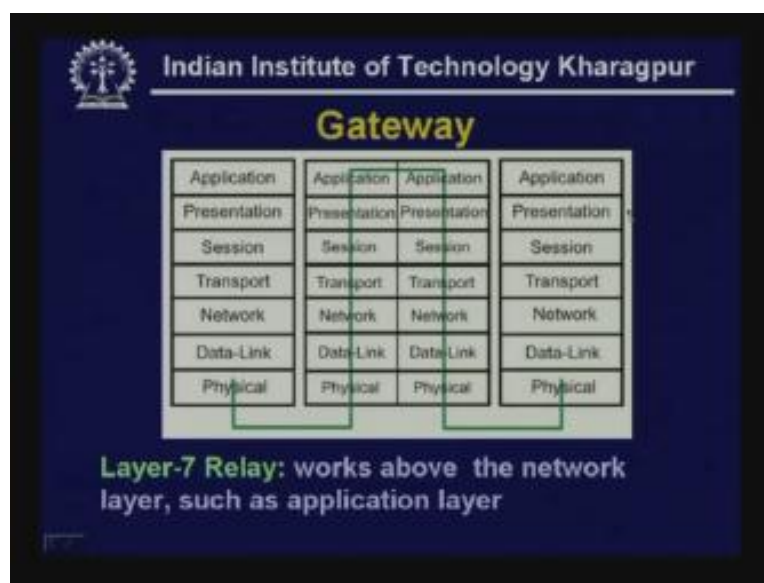
A bridge is essentially a layer - 2 relay which links similar or dissimilar LANs. That means with the help of this bridge you can connect two Ethernet LANs or one Ethernet one say token ring LAN so two similar or dissimilar LANs can be connected. here we are not really extending a single LAN so two dissimilar LANs are connected or two similar LANs two Ethernet LANs are connected with the help of a bridge and it operates in data link layer as you can see so this is one side and this is another side (Refer Slide Time: 51:23) which are linked, this is one user and this is another user so this is linked with the bridge. As you can see the frame goes from this side to this side through a bridge which operates in two layers. So it is designated to perform store and forward frames. So it receives it and then it does some error checking and other things and then forwards it. So it is protocol independent and transparent to end stations.

(Refer Slide Time: 52:40)



On the other hand, a layer - 3 relay which links dissimilar networks acts on network layer frames not transparent to the end stations. That means it can modify the contents of the frame, it can change the addresses so it is not really transparent to the end stations, it isolates LAN into subnets to manage and control network traffic. So these routers are very important functions. They are linked with help of these kinds of devices these are nothing but routers (Refer Slide Time: 52:36).

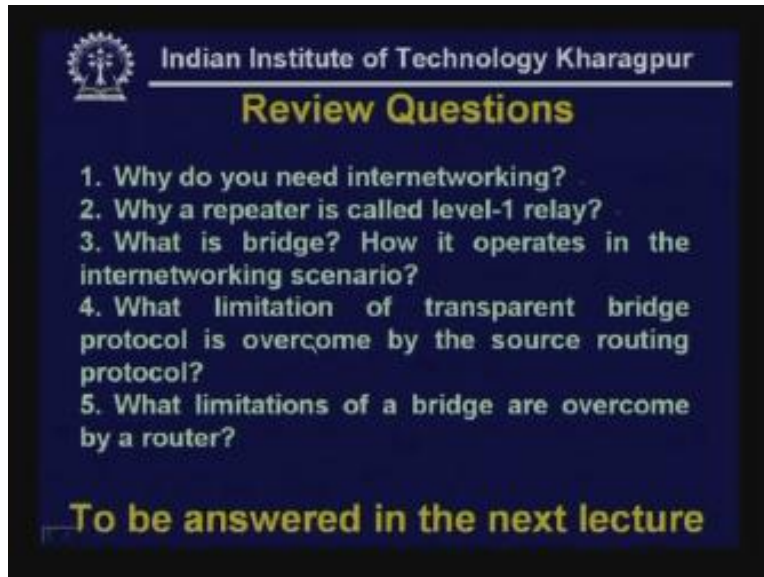
(Refer Slide Time: 53:10)



Finally this is the gateway as I mentioned which works above the network layer such as application layer. So here you see the gateway operating in application layer and two

systems are connected through a gateway and the communication is performed. It goes all the way up to the application layer and then it comes down and goes to the other side. So this is how the gateway works.

(Refer Slide Time: 53:49)

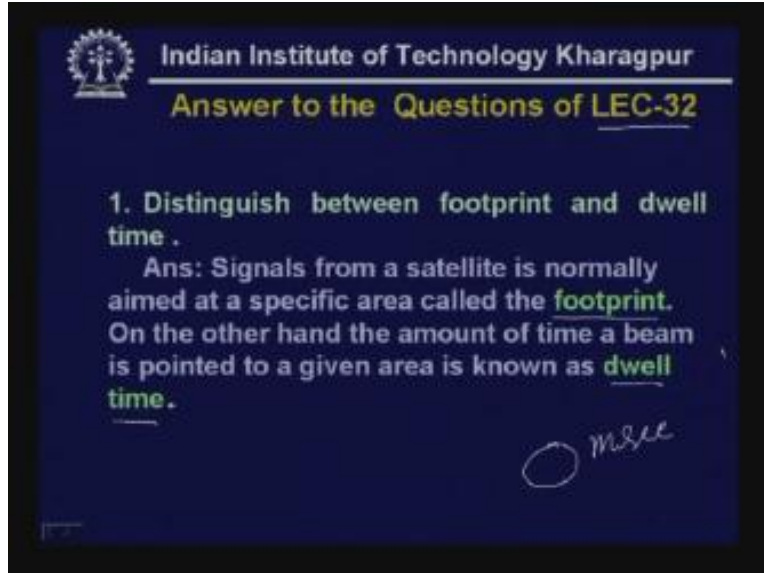


Now it is the time to give you the review questions.

- 1) Why do you need internetworking?
- 2) Why a repeater is called the level one relay?
- 3) What is bridge how it operates in the internetworking scenario?
- 4) What limitation of transparent bridge protocol is overcome by the source routing protocol?
- 5) What limitations of a bridge are overcome by a router?

These are the 5 questions based on this lecture to be answered in the next lecture.

(Refer Slide Time: 54:33)



Indian Institute of Technology Kharagpur
Answer to the Questions of LEC-32

1. Distinguish between footprint and dwell time .

Ans: Signals from a satellite is normally aimed at a specific area called the **footprint**. On the other hand the amount of time a beam is pointed to a given area is known as **dwell time**.

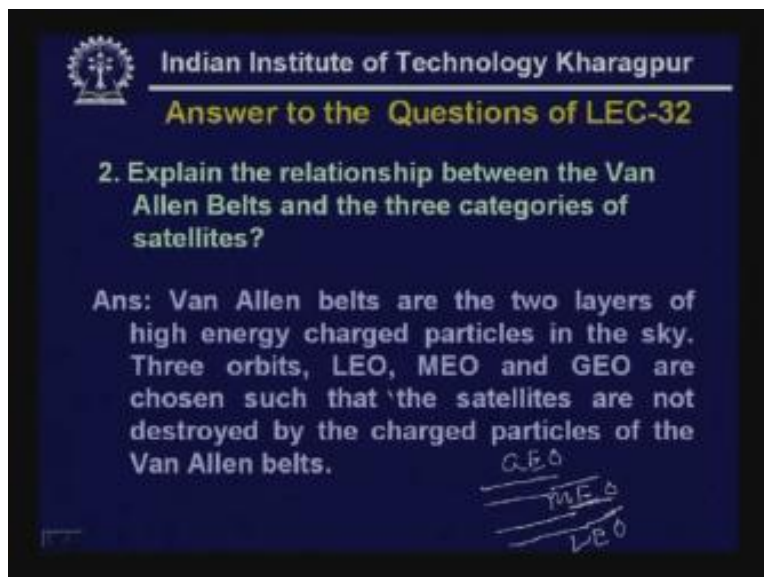
msc

Here are the answers to the questions of lecture – 32.

1) Distinguish between footprint and dwell time?

Signals from a satellite are normally aimed at a specific area called the footprint so it covers a large area. On the other hand, the amount of time a beam is pointed to a given area is known as dwell time. That means a satellite can focus its beam for some duration which is of the order of millisecond for transfer of data or for data communication then it focuses on some other path, so this is known as the dwell time.

(Refer Slide Time: 55:29)



Indian Institute of Technology Kharagpur
Answer to the Questions of LEC-32

2. Explain the relationship between the Van Allen Belts and the three categories of satellites?

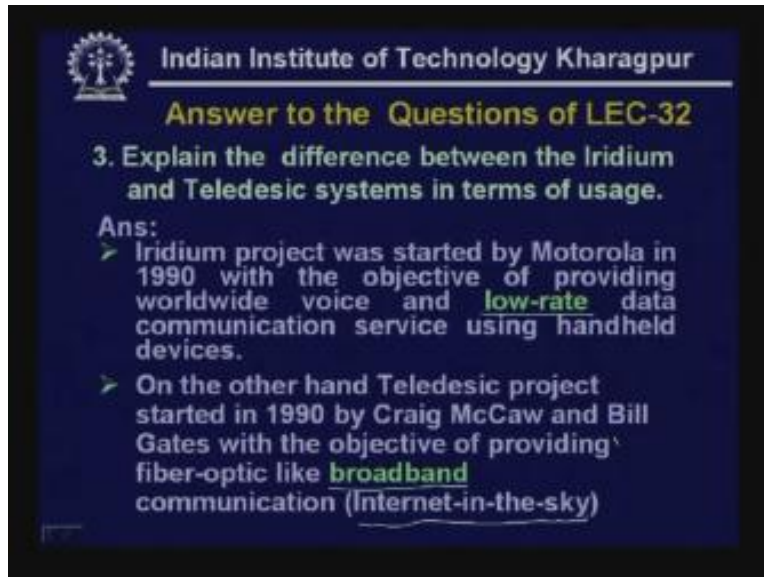
Ans: Van Allen belts are the two layers of high energy charged particles in the sky. Three orbits, LEO, MEO and GEO are chosen such that the satellites are not destroyed by the charged particles of the Van Allen belts.

*GEO
MEO
LEO*

2) Explain the relationship between the Van Allen belts and the three categories of satellites.

Van Allen belts are the two layers of high energy charged particles in the sky. We have seen there are two layers of Van Allen belts. There are three orbits LEO, MEO and GEO which are positioned above or below these three layers. They are chosen in such a way that the satellites are not destroyed by the charged particles of the Van Allen belts. So this is the relationship between the different types of orbit and the Van Allen belts.

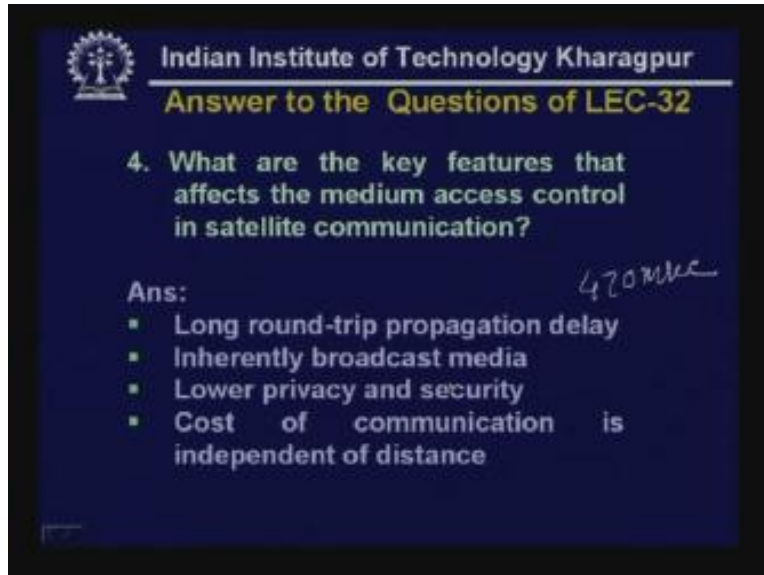
(Refer Slide Time: 56:14)



3) Explain the difference between the Iridium and the Teledesic system in terms of usage.

Iridium project was started by Motorola in 1990 with the objective of providing worldwide voice and low rate data communication service using handheld devices. On the other hand, Teledesic project was started in 1990 by Craig McCaw and Bill Gates with the objective of providing fiber optic like broadband communication. From here you can see these are the two differences for communication. So, essentially this Teledesic system was deployed to provide **internet in the sky**.

(Refer Slide Time: 56:43)



Indian Institute of Technology Kharagpur
Answer to the Questions of LEC-32

4. What are the key features that affects the medium access control in satellite communication?

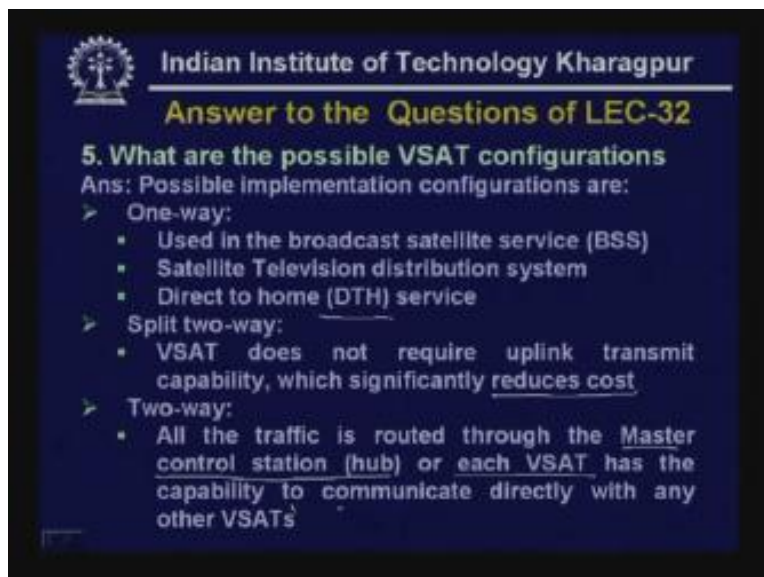
Ans: *470 msec*

- Long round-trip propagation delay
- Inherently broadcast media
- Lower privacy and security
- Cost of communication is independent of distance

- 4) What are the key features that affect the medium access control in satellite communication?

There are four features; long round-trip propagation delay which is about 470 millisecond, inherently broadcast media, low privacy and security, and the cost of communication is independent of distance. So these are the four features that you have to take into consideration.

(Refer Slide Time: 57:23)



Indian Institute of Technology Kharagpur
Answer to the Questions of LEC-32

5. What are the possible VSAT configurations

Ans: Possible implementation configurations are:

- One-way:
 - Used in the broadcast satellite service (BSS)
 - Satellite Television distribution system
 - Direct to home (DTH) service
- Split two-way:
 - VSAT does not require uplink transmit capability, which significantly reduces cost
- Two-way:
 - All the traffic is routed through the Master control station (hub) or each VSAT has the capability to communicate directly with any other VSATs

5) What are the possible VSAT configurations?

Possible implementation configurations are one-way used in broadcast satellite services for example direct to home service which are used nowadays, satellite television distribution system split two-way in this case VSAT does not require uplink transfer capability which significantly reduces the cost. Two-way is very popular, all the traffic is routed through either master control station or each VSAT has a capability to communicate directly with each other or with any other VSATs. With this we conclude today's lecture, the next two lectures will be on TCP/IP, thank you.